• A Tracker in your Pocket •

Fundación Karisma

Executive Summary

Since 2011, the Colombian government has tried to solve the cellphone theft problem with the cellphone registry.[1] The idea behind the system set forth by the national government and the telecom regulator (called CRC) is to block cellphones when reported as stolen or lost, using a unique identifier number called IMEI. Ideally, the fact that a cellphone is blocked —and therefore rendered unusable in Colombian networks— should deter theft. However, the system as it exists currently exceeds that purpose. Furthermore, it affects fundamental rights such as privacy and freedom of expression in a way that is unjustifiable even if the system turns out to be effective.

The report ***A tracker in your pocket*** presents an analysis of the cellphone registry in Colombia. This analysis is composed of three main parts:

1. A basic description of how the registry works.
2. Problematic aspects of the registry.
3. Conclusions and recommendations to the main actors involved in the registry: CRC, Ministry of ICT, Data Protection Authority and mobile carriers.

1 This system is structured by Article 106 of Law 1453/2011, Decree 1630/2011 and Telcom Regulator (CRC) Resolution 3128/2011.

How does the registry work?
Basic elements of the cellphone registry

IMEI and databases

IMEI stands for International Mobile Equipment Identity and it is a unique number assigned to each cellphone. Mobile carriers can use this number to know which device uses the network. When a person reports his/her cellphone as being stolen or lost, the mobile carrier registers the device's IMEI in a particular database, called ***negative operative database***, and denies further access to the network from that reported IMEI. As a consequence, the cellphone cannot send or receive calls and text messages.

Additionally, everyone must register their personal information when buying a cellphone. Then, mobile carriers keep that information associated to the device's IMEI, the subscriber number (called IMSI), and the line number (or MSISDN). All information is stored on a database called ***positive operative database.***

The registry system has yet another type of database called ***administrative database***, and it is currently operated by El Corte Inglés, a company of Spanish origin. This organization carries two types of databases: negative and positive. The first one, called ***Negative Administrative Database***, keeps all reported IMEIs and shares them with all mobile carriers even if they were reported to another carrier. In this way, every carrier has a list (database) of all reported cellphones. The second one, called ***Positive Administrative Database***, keeps track of all the positive databases that mobile carriers have.

Verification procedure

To make sure no cellphone reported on the negative database connects to the network, the system has a verification procedure divided into two stages or cycles. Initially, the procedure catches reportedly stolen IMEIs along with IMEIs that do not comply with technical standards, IMEIs not registered on the positive databases, or cases in which the IMEIs might have been duplicated. In other words, it picks up irregular IMEIs connecting to the network.

To make this verification possible, mobile carriers must analyze sensitive information of their users. This information is stored on the ***Charge Detail Records*** (CDR) and it can show who is contacted, when, for how long, from where, etc. In detail, the telecom regulator orders mobile carriers to analyze mainly:

- Sender and receiver numbers
- Location of the call or data session
- Time and duration of a call or data session
- IMEI
- IMSI

According to the procedure, when an irregular IMEI is detected, the carriers must block it.

Problematic aspects of the registry

The framework of this analysis is human rights standards and impact, specifically, the United Nations and Inter-American System of International Human Rights Law, the Colombian Constitution and The International Principles on the Application of Human Rights to Communications Surveillance[2].

The problems this registry represents for the rights to privacy and freedom of expression are analyzed based on the elements of the system (i.e. databases and verification procedure). Finally, some remarks are made about the registry in general.

Problems associated with the databases

Each IMEI is tied to a person: Because of the way the system works, each IMEI is equivalent to a person's identity. These registry mechanisms have been rejected by the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression of the United Nations because they eliminate the possibility to communicate anonymously. They allow the tracking of people and they simplify the surveillance of communications.

Authorities' Access: According to Resolution 3128, any authority can access IMEI databases' information. However, according to the Constitution, it is clear that this access must be authorized by a judicial authority and only for criminal investigation procedures. In any case, it is problematic that the Ministry of ICT and the telecom regulator have established such a broad and ambiguous regulation to access the information.

Precisely, the abuse of this information is the main danger people in Colombia face with the implementation of the cellphone registry. In

2 The International Principles on the Application of Human Rights to Communications Surveillance. (2014, May 10). Available at: https://necessaryandproportionate.org/about

Mexico a similar system was created, however, in 2011 it was eliminated because personal information, as well as metadata, was being sold and used for illegal purposes in cases of extortion and abduction. In Ukraine, people attending a protest in 2014 received a text message that said: "Dear subscriber, you are registered as a participant in a mass riot." In Colombia, with this system, authorities can not only obtain cellphone numbers of people gathered in a certain place but they can obtain their names, identity numbers and physical addresses, among other information, because they would have a database that can relate a cellphone's technical data with the personal information of its owner.

Problems associated with the verification procedure

The verification procedure uses very sensitive data about users' communication called *metadata*, that is contained on Charge Detail Records (CDR). This data reveals to whom, when, where, and for how long someone communicates with a contact. Because of its nature, metadata can be used to create complete profiles of the activities and preferences of a person.[3]

Because of its importance, it has been internationally recognized that collection and conservation of metadata is a limitation to the right of privacy. It is important to protect this information because it can reveal patterns and give an idea of someone's behaviour[4], especially when various information sources can be crossed and aggregated[5]. Therefore, it is necessary to consider that production and retention of communications metadata augment the state's surveillance capabilities and, by the same way, the possibility of abuse of this information[6].

The regulation of the cellphone registry does not take into account the context of the surveillance of communications. Therefore, risks to privacy and freedom of expression were not considered. In Colombia, there are measures like communications interception and data reten-

---

3 The International Principles on the Application of Human Rights to Communications Surveillance. Op. Cit.

4 The High Commissioner for Human Rights of the United Nations on its report *The right to privacy in the digital age* has pointed out that, in the context of the right to privacy, "The aggregation of information commonly referred to as "metadata" may give an insight into an individual's behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication. As the European Union Court of Justice recently observed, communications metadata "taken as a whole may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained."5 Recognition of this evolution has prompted initiatives to reform existing policies and practices to ensure stronger protection of privacy." Human Rights Council (2014, June 30). P.19.

5 Human Rights Council, op cit, (note 3), par. 15.

6 Ibid. par.67.

tion for mobile lines that are not compliant with the mentioned rights[7]. Nevertheless, those measures use communications metadata without adequate controls to avoid the abuse of these powers.

The Constitution, which prevails over any other legal norm, demands that access to private communications must be made only under a law that (1) allows the interception, (2) creates a procedure to carry the interception, and if (3) a judge legalizes the procedure.[8]

The same protection recognized for communication's content must be granted to metadata. Because of these reasons, only the Prosecutor's Office can order access to the databases of the cellphone registry, for the sole purpose of evidence collection during a criminal investigation. This activity requires judicial authorization. Any other intervention on personal communication is unconstitutional.[9]

Problems of the registry in general

The cellphone registry in Colombia is designed in such a way that responsibility for the system falls on a third party, El Corte Inglés. This company only has a formal relationship with mobile carriers and it is governed by a private contract. Therefore, it is not initially subject to the same controls that public entities are and thus has reduced transparency and democratic control.

Another effect of this system is that neither the Ministry of ICT nor the CRC knows the contract between El Corte Inglés and mobile carriers. If the contract is not known by any authority, the system is clearly being developed without oversight, in spite of the broad powers that these authorities have, especially the Ministry of ICT[10].

'Additionally, while the law directs the CRC to operate in a system aimed at reducing theft, it should be noted that the regulator, is by design, in charge of the promotion of the competition on telecommunications.[11]

---

7 More on communications surveillance in Colombia: Cortés, C. (2014). Vigilancia de las comunicaciones en Colombia. Bogotá, Colombia: Dejusticia, 18; Rivera, J.C. y Rodríguez, K. (2015). Vigilancia de las comunicaciones por la autoridad y protección de los derechos humanos en Colombia. San Francisco, EEUU: Electronic Frontier Foundation; Castañeda, J.D. (2016). ¿Es legítima la retención de datos en Colombia?. Bogotá, Colombia: Fundación Karisma; Pérez, G. (2016). Hacking Team: malware para la vigilancia en América Latina. Santiago, Chile: Derechos Digitales

8 Colombian Constitution. Article 15. Constitutional Court (1993). Ruling T-349. Available at: http://www.corteconstitucional.gov.co/relatoria/1993/T-349-93.htm

9 For example, CRC demands mobile carriers to hand over CDR of their users. See CRC Resolution 3128 of 2011, article 10.a.9, lit. b y d.

10 Law 1341 of 2009. Article 4.

11 Ibid.

Conclusion: The cellphone registry is not proportional

The cellphone registry seeks to reduce cellphone theft. However, there are various reasons why the program does not fulfill its purpose and, instead, represents a violation of rights to privacy and freedom of expression.

The registry does not work because, after being blocked, a cellphone can be sold by pieces. The blocking only affects the network functions of the device, which means that it retains the value and usefulness of a music player, tablet or internet calling device.

> The system has been modified repeatedly to ensure that no irregular cellphone works over the Colombian mobile networks. Nevertheless, there will always be devices that escape control because IMEIs can be reprogrammed. Also it is possible to sell the device by pieces or use its other capabilities to take pictures, listen to music, record files or even make voice calls if connected to WiFi, activity against which the registry cannot do anything.

Even if the registry was effective, the restriction to rights to privacy and freedom of expression is not proportionate.[12] The Colombian cellphone registry has grown uncontrolled as a technical solution. Instead of such an invasive program, the policy could be focused on using the voluntary reporting of cellphone theft to build the negative list along with national and international cooperation by carriers to block reported devices, as well as capturing criminal groups engaged in this activity. This would be as effective and less invasive than the current registry.

From the international standards of human rights protection, it is clear that **the system is not legal nor it is proportional, in spite of having a legal objective.**

12 According to official numbers, cellphone theft has increased since 2011, the year the cellphone registry system was introduced. The Statistical Criminal Information System (SIEDCO in Spanish) reported more than 32 thousand thefts for 2011. This number has reached 52 thousand cases in 2015. See also: Roa, L. (2016). Extinción de dominio como herramienta contra el hurto de celulares en la ciudad de bogotá. Revista Criminalidad, 58 (2): 157-174. Available at: http://www.scielo.org.co/pdf/crim/v58n2/ v58n2a06.pdf.

Recommendations

The cellphone registry in Colombia is illegal, based on the previously reviewed reasons. However, the legal framework is in force until a judge decides that it is not. Considering the impact of the system on peoples' rights, the CRC and Ministry of ICT may eliminate and modify certain parts of the system.

CRC

The CRC has a restricted role on the registry system. It can, however, override some problematic implementations such as the association between IMEI, IMSI and telephone number; the carrier's duty to verify users' identity against the National Registry Office and risk centrals; and the access to databases by any authority, without controls and rationale for this access.

The CRC can also derogate the verification procedure and the part of the regulation that allows itself to access the communications metadata.

Ministry of ICT

The Ministry can derogate the portion of Decree 1630 of 2011 related to the databases and verification procedure. The Ministry can propose to Congress to overturn article 106 of Law 1453/2011 which assigns the regulation function to CRC.

Additionally, the Ministry must think about public policy related to technologies from a human rights perspective, especially taking into account the impact on the right to privacy and freedom of expression. The Ministry can ask the Interamerican Court of Human Rights for support and solicit an opinion about compatibility of this registry with the American Convention on Human Rights and International Covenant on Civil and Political Rights[13].

Finally, the Ministry must reinforce alternatives to the cellphone registry that do not affect rights to privacy and freedom of expression disproportionately.

13 American Convention on Human Rights. Article 64. Num. 2. Rules of Procedure of the Interamerican Court of Human Rights. Article 72.

Data protection authority

The Authority must participate in the government's initiatives related to personal data collection and use. This participation must be focused on the protection of privacy and habeas data rights.

Mobile carriers

Mobile carriers must check requests by authorities regarding access to communications information and accept only those that comply with constitutional and legal requirements. Carriers must state clearly on their transparency reports which information is being requested by which authorities, why are they requesting this information, and if the mobile carrier accepted or rejected the request.

Finally, they must consider human rights on behalf of their users over policy discussions with the government and the regulator, as some providers have done during the regulation process.

Want to learn more?

Fundación Karisma has launched a research report along with the website karisma.org.co/nomas-celusvigilados to explain the cellphone registry in Colombia and its problems. Most of the material is in Spanish, still you will be able to find two key pieces in English: an animated video called The war against phone theft in Colombia and this executive summary of Karisma's research. Read and share!